HOW TO OPTIMISE YOUR SIEM

A COMPREHENSIVE GUIDE

WWW.RIVERSAFE.CO.UK

RIVERSAFE

CONTENTS

EXECUTIVE SUMMARY

In cybersecurity, the need for optimised and efficient Security Information and Event Management (SIEM) systems has never been more crucial. These systems serve as the cornerstone for many organisations' security postures, offering real-time analysis of security alerts generated across various applications and networks. However, the secret to unlocking the maximum potential of these systems lies not just in their implementation, but more importantly, in their optimisation.

This white paper takes an in-depth look into the crucial aspect of SIEM optimisation, an area often overshadowed by the initial implementation process.

We start by clarifying the concept of SIEM optimisation, setting it apart from SIEM implementation.

We then dive into the tangible benefits and advantages of a properly optimised SIEM. These include improved threat detection and response, a reduction in false positives, more efficient use of security resources, and overall cost-effectiveness.

The core of this paper presents seven key strategies for achieving effective SIEM optimisation. These strategies encompass fine-tuning rules to reduce noise and false alarms, integrating and leveraging threat intelligence for enhanced, proactive security, expanding log source coverage to ensure comprehensive visibility, conducting regular health checks to maintain system performance, optimising data storage and processing for cost management and speed improvement.

Additionally, it highlights the importance of developing and implementing an effective automation and orchestration strategy, and the importance of data normalisation and enrichment in enhancing the accuracy and efficiency of your SIEM system.

Beyond these strategies, this guide provides a set of best practices for ongoing SIEM optimisation. These practices offer a roadmap for maintaining the efficiency and effectiveness of your SIEM system over time, helping to ensure that it continues to deliver value in the face of evolving threats and changing business requirements.

In summary, this white paper offers a comprehensive guide to understanding and implementing SIEM optimisation, providing valuable insights and practical strategies to enhance your organisation's cybersecurity posture. Let's dive in.

UNDERSTANDING SIEM OPTIMISATION

While both SIEM implementation and optimisation are crucial, they have distinct roles and occur at different stages in the SIEM lifecycle.

SIEM implementation is the initial setup phase. It involves installing the SIEM software, configuring the system in line with the organisation's IT environment, setting up initial rules and policies, and integrating the system with existing applications and infrastructure. The goal at this stage is to establish a functioning system that can start providing immediate value.

SIEM optimisation is an ongoing, dynamic process that ensures the SIEM system remains effective, efficient, and aligned with an organisation's security needs. This involves refining the SIEM's configuration, rules, and policies, ensuring the system is updated with the latest threat intelligence, expanding log sources as the organisation's IT landscape evolves, and conducting routine health checks for optimal performance.

Notably, the process of optimisation requires a deep understanding of the organisation's security posture, threat landscape, and IT infrastructure. It also demands an appreciation of the SIEM system's capabilities and limitations. This knowledge allows for informed adjustments and enhancements to the SIEM system, facilitating improved threat detection and response, and ensuring valuable IT resources are not wasted on false positives or unnecessary activities.

THE BENEFITS OF A WELL OPTIMISED SIEM

A well-optimised SIEM system offers numerous benefits to an organisation. Here are the key advantages:

- **Cost Savings:** By improving efficiency, reducing false positives, and speeding up incident response times, a well-optimised SIEM aids in substantial cost savings, avoiding the financial damages associated with security breaches and reducing the operational costs of the security team.
- **Improved Threat Detection and Response:** A finely tuned SIEM system effectively identifies and promptly responds to a wide array of security threats, improving the overall security posture of the organisation.
- **Enhanced Threat Intelligence:** The system effectively processes and analyses log data from various sources, providing actionable threat intelligence. This enables proactive identification and mitigation of potential threats.
- **Improved Incident Response Times:** Optimised rules and alerts enable the SIEM system to quickly detect security incidents and trigger immediate responses, significantly limiting potential damage.
- **Reduced False Positives:** Fine-tuning the rules and alerts drastically reduces the number of false positives, allowing security teams to focus on genuine threats.
- **Enhanced Operational Efficiency:** SIEM optimisation aids in streamlining security operations by automating routine tasks and refining workflows, allowing teams to focus on strategic activities.
- **Better Compliance Management:** A well-optimised SIEM provides detailed reports and real-time visibility into the IT environment, making it easier to meet compliance requirements and identify potential compliance issues early.

The advantages of a well-optimised SIEM system are multi fold. In addition to enhancing an organisation's defence against cyber threats, an optimised SIEM impacts operational efficiency and regulatory compliance. It is a vital tool that, when properly managed and optimised, can contribute significantly to the organisation's overall cyber resilience strategy.

5 CORE STRATEGIES TO OPTIMISE YOUR SIEM:

STRATEGY NO #1: PERFORMING REGULAR HEALTH CHECKS

Regular health checks are a crucial part of maintaining the effectiveness of your SIEM system. They help ensure that your SIEM is operating as expected, and highlight areas where improvements can be made.

STEPS FOR PERFORMING REGULAR HEALTH CHECKS

- **Check System Status:** Regularly check the status of your SIEM system. This includes checking for any error messages, system alerts, or other indications of problems.
- **Monitor System Performance:** Keep an eye on the performance of your SIEM system. This includes tracking metrics like CPU usage, memory usage, disk space usage, and network bandwidth usage. If you're using a cloud-based SIEM solution, the service provider generally manages system performance and rectifies issues as they arise. However, for on-premise solutions, monitoring CPU and memory usage is particularly crucial, as system resources are more directly tied to performance.
- **Review Log Source Status:** Regularly review the status of your log sources. Make sure that all log sources are active and sending data to your SIEM. If any log sources are inactive, troubleshoot to identify and resolve the issue.
- **Check Rule Performance:** Review the performance of your SIEM rules. Look for any rules that are generating a large number of false positives, or that are not triggering when they should. Adjust your rules as needed to improve their accuracy and effectiveness.
- **Test Incident Response:** Periodically test your incident response process. This can help you identify any issues or inefficiencies in your response process, and ensure that your team is prepared to respond effectively to real incidents.
- **Review System Configuration:** Regularly review the configuration of your SIEM system. Look for any misconfigurations that could be impacting system performance or effectiveness.

By performing regular health checks on your SIEM, you can ensure that your system is operating efficiently and effectively, and proactively address any issues before they impact your security posture. Regular health checks also provide an opportunity to continuously improve your SIEM system, by identifying areas for improvement and making the necessary adjustments.

SAMPLE SIEM HEALTH CHECK CHECKLIST

To streamline this process, consider using a health check checklist. This tool can help you track your regular tasks, their frequency, and their status. It can also be invaluable for recording any issues you've identified and the steps you've taken to resolve them. Here's an example:

TASK	FREQUENCY	LAST CHECKED	STATUS	NOTES
Check System Status	Daily	2023-09-30	Completed	No issues found
Monitor System Performance	Daily	2023-09-30	Completed	CPU usage high, needs investigation
Review Log Source Status	Weekly	2023-09-27	Completed	Log source #3 inactive, resolved
Check Rule Performance	Monthly	2023-09-01	Completed	Rule #7 generating false positives, adjusted
Test Incident Response	Quarterly	2023-09-01	Completed	Response time improved
Review System Configuration	Monthly	2023-06-01	Completed	No misconfigurations found

This checklist can be modified to fit the specific needs and scale of your organisation. The frequency of each task can be adjusted based on the complexity of your SIEM environment, the resources available, and the sensitivity of the data and devices involved.

The ultimate goal of these health checks is to ensure that your SIEM system is functioning optimally and effectively protecting your network. Regular health checks and corresponding adjustments can significantly enhance the performance and reliability of your SIEM system.

Schedule your SIEM Health Check today

STRATEGY NO #2: OPTIMISING DATA STORAGE AND PROCESSING

Optimising data storage and processing is an essential step in fine-tuning your SIEM system. Proper management of data storage can have a significant impact on the performance of your SIEM, efficient data processing is necessary for timely and accurate threat detection and response. Below are some strategies to consider:

STRATEGIES FOR OPTIMISING DATA STORAGE AND PROCESSING

- **Data Retention Policies:** Implement and enforce data retention policies. This can help manage the volume of data your SIEM needs to store and process, reducing storage needs and improving performance. Remember to comply with any legal or regulatory requirements related to data retention.
- **Data Compression and Archiving:** Use data compression techniques to reduce the size of your stored data. Also, consider archiving older data that is not immediately needed for analysis but may be needed for long-term investigations or compliance purposes.
- **Efficient Data Parsing and Normalisation:** Ensure efficient data parsing and normalisation processes. This will help your SIEM system to accurately identify and categorise incoming data, improving its ability to detect threats and reducing the likelihood of false positives.
- **Scalable Infrastructure:** Use a scalable infrastructure to handle increases in data volume. This could involve using cloud storage solutions or scaling out your SIEM infrastructure to meet increased demand.

CATEGORIES OF DATA STORAGE OPTIONS FOR SIEM SYSTEMS

By optimising your data storage and processing, you enhance your SIEM system's ability to swiftly parse and analyse incoming data, leading to quicker threat detection and response. An efficient data management strategy allows for precise categorisation and prioritisation of data, reducing false positives and focusing attention on genuine threats.

CATEGORY	DESCRIPTION	USE CASES	SUGGESTED STORAGE MEDIUM
Hot Storage	This is where active, frequently accessed data is stored. It is readily available for analysis and reporting.	Real-time threat detection, immediate incident response	Enterprise-grade NVMe SSDs for the fastest data retrieval speeds.
Warm Storage	This is used for less frequently accessed data that is still needed fairly quickly. It provides a balance between cost and speed.	Short-term data analysis, regular reporting	Enterprise-grade SATA SSDs or SAS HDDs which provide a balance between speed and cost.
Cold Storage	This is the most cost-effective storage option, used for data that is infrequently accessed. Retrieving data from cold storage can be slower.	Long-term data retention, compliance requirements, historical analysis	High-capacity, energy-efficient SATA HDDs or cloud-based cold storage services like Amazon S3 Glacier.
Archived Storage	This is used for data that is no longer needed for regular access but needs to be retained for a long period, often for compliance reasons. The data is often offline and retrieval can take considerable time.	Compliance requirements, long-term archival	Offline storage like tape drives, or cloud-based archival services like Amazon S3 Glacier Deep Archive.

STRATEGY NO #3: FINE-TUNING CORRELATION RULES

To effectively identify potential security incidents, SIEM systems heavily rely on correlation rules. These rules, essentially conditions or patterns that the system checks within the log data, form the bedrock of a SIEM system's functionality.

However, the potency of these rules hinges on their alignment with the specific context of your organisation, including factors such as your organisation's risk profile, network architecture, and security policy.

ACTIONS TO FINE-TUNE CORRELATION RULES

- **Understand Your Organisation's Context:** Understand the particularities of your organisation's risk profile, network architecture, and security policy. This understanding forms the basis for effective rule tuning.
- **Review Existing Rules:** Regularly review your existing correlation rules. Ensure they align with your current risk profile and IT environment.
- **Address False Positives:** If you notice a high rate of false positives, consider adjusting the correlation rules to be more precise. This can involve tightening conditions or incorporating additional factors.
- **Set Alert Thresholds:** Establish thresholds for alert generation. This can prevent the system from raising alarms for minor events that do not pose a significant risk.
- **Define Composite Events:** Consider defining composite events, which are complex events consisting of multiple individual events. These can provide a more nuanced view of activity in your network.
- **Incorporate Time-Based Conditions:** Include time-based conditions in your rules. The timing of an event can often be a significant factor in assessing its importance.

CHECKLIST FOR FINE-TUNING CORRELATION RULES

By following these steps and using this checklist, you can ensure that your SIEM system's correlation rules are as precise and effective as possible. This reduces "noise" in the system and allows security analysts to focus on genuine threats, thereby maximising the system's threat detection accuracy and providing reliable intelligence for your security team.

CHECKLIST ITEM	DONE
Understand your organisation's risk profile, network architecture, and security policy	☐
Review and update the correlation rules	☐
Ensure the rules align with the current IT environment and risk profile	☐
Adjust rules that were generating too many false positives	☐
Set appropriate thresholds for alert generation	☐
Define relevant composite events	☐
Incorporate time-based conditions into the correlation rules	☐

STRATEGY NO #4: INTEGRATING AND LEVERAGING THREAT INTELLIGENCE

Threat intelligence feeds can significantly enhance your SIEM's detection capabilities. They provide a wealth of contextual information in the form of known malicious IP addresses, URLs, file hashes, and other indicators of compromise (IOCs).

By integrating these feeds into your SIEM system, you can correlate this information with your existing event data, thereby enhancing the system's ability to identify potential threats.

ACTIONS FOR INTEGRATING AND LEVERAGING THREAT INTELLIGENCE

- **Identify Threat Intelligence Sources:** Due to the availability of various threat intelligence sources, it's important to identify the most relevant ones based on your organisation's need and threat landscape.
- **Integrate Threat Intelligence Feeds:** Incorporate the selected threat intelligence feeds into your SIEM. This might involve using an API or a data import function depending on your SIEM's capabilities.
- **Correlate Threat Intelligence with Event Data:** Ensure that your SIEM is correlating the IOCs from the threat intelligence feeds with your existing event data. This will help the system to identify and alert on potential threats more accurately.
- **Update Threat Intelligence Regularly:** Threat intelligence is continually evolving, so it's important to ensure your feeds are updated regularly to keep up with the latest threats.
- **Review and Adjust Correlation Rules:** Review your correlation rules to ensure they are making use of the threat intelligence data. Adjust the rules as necessary based on the intelligence received.

LIST OF THREAT INTELLIGENCE VENDORS

The following table provides some examples of threat intelligence vendors. There are, however, hundreds of threat intelligence feeds and vendor offerings available in the market. The choice of which to use will depend on your organisation's specific needs and threat landscape.

VENDOR	TYPE OF INTELLIGENCE	DESCRIPTION
DomainTools	Domain Risk Score, Threat Profile	Offers threat intelligence services focusing on domains, including risk scoring and threat profiling.
AlienVault OTX (Open Threat Exchange)	IP Reputation, Malware	Provides a free threat intelligence feed that includes data on IP reputation, malware, and other threats.
ThreatQ	Broad Range	Provides a threat intelligence platform that helps organisations manage and triage threats.
AWS	Broad Range	AWS offers a variety of threat intelligence services including GuardDuty, which provides threat detection.
Palo Alto	Broad Range	Provides a platform that includes threat intelligence to prevent known and unknown threats.
Abuse.ch	Fraudulent IPs, Malware	An open threat intelligence feed providing information about suspected fraudulent IPs and malware.
Cisco	Broad Range	Cisco offers a range of threat intelligence services through its security products.
Spamhaus	IP Reputation, Spam	Specialises in providing real-time threat intelligence for spam and malware.
PhishTank	Phishing	An open community that provides a free threat intelligence feed dedicated to phishing data.

STRATEGY NO #5: ENHANCING USE CASE DEVELOPMENT

Enhancing use case development plays a pivotal role in optimising your SIEM system. The effectiveness of your SIEM is directly linked to the quality of use cases you create. Developing well-defined use cases will bolster your SIEM's capability to identify and respond to security threats effectively.

STEPS FOR ENHANCING USE CASE DEVELOPMENT

- **Identify Potential Use Cases:** Start by identifying potential security use cases that align with your network's security needs. These could encompass areas such as intrusion detection, unauthorised access, data breaches, and more.
- **Prioritise Use Cases:** Not all use cases hold equal importance. Prioritize them based on the criticality of the threats they address, the impact on your network, and their relevance to your security posture.
- **Implement Use Cases:** Implement each use case by configuring your SIEM system to monitor and alert on specific security events. This might involve setting up custom rules, triggers, or alerts, depending on your SIEM's capabilities.
- **Validate Use Case Effectiveness:** After implementing a new use case, validate that your SIEM is correctly identifying and responding to security events as intended.
- **Maintain and Evolve:** Regularly review and update your use cases to ensure they remain relevant and effective. Adjust them as your network's security landscape evolves.

Enhancing use case development is pivotal for maximising your SIEM's threat detection capabilities. By focusing on use cases, you can fine-tune your SIEM to precisely target the security issues that matter most to your organisation. Keep in mind that a balance must be struck between the number of use cases and their effectiveness to avoid overwhelming your SIEM with excessive data.

SAMPLE ASSET INVENTORY CHECKLIST

To assist with this process, consider utilising an asset inventory checklist. This tool helps you assess and track your organisation's assets, prioritise them based on criticality, and monitor the configuration and validation status of each log source. Here's a sample:

ASSET ID	ASSET TYPE	ASSET NAME	LOCATION	OWNER	LOG SOURCE VALIDATED
001	Server	Web Server 1	Data Centre 1	John Doe	Yes
002	Database	Customer DB	Data Centre 2	Jane Doe	Yes
003	Firewall	Main Firewall	Office 1	Bob Smith	Yes
004	Workstation	Marketing Workstation	Office 2	Alice Johnson	No
005	Application	HR Software	Cloud	Charlie Brown	No
006	Network Device	Core Switch	Data Centre 1	David Johnson	Yes

In the context of managing a comprehensive asset inventory, a configuration management database (CMDB) can prove to be an invaluable resource. A CMDB is a centralised system that encompasses the entire IT environment. It enables the monitoring, tracking, and management of your IT assets in one place. A CMDB is a popular choice among IT professionals as it not only stores data about your configurable items (CIs) but also helps to better understand the relationships between these items.

Following the asset inventory checklist, it's important to note that your inventory doesn't have to be as comprehensive as the example provided. The checklist is intended to be a guide, and your actual inventory can be adjusted to meet your organisation's specific needs.

The primary goal of the asset inventory is to ensure you're achieving sufficient log source coverage across your network. This isn't necessarily about having a large number of log sources, but rather about having the right log sources. Here are some things to consider:

- **Critical Assets:** Make sure your critical assets are included as log sources. These are the systems, applications, and devices that are most crucial to your organisation's operations or that handle sensitive data.
- **Diversity of Log Sources:** Aim for a diverse set of log sources. This includes servers, network devices, applications, databases, etc. Diversity in your log sources provides a more holistic view of your network activity.
- **Compliance and Storage Requirements:** Understand the compliance requirements of your log sources. Certain assets or types of data may have specific compliance regulations that dictate how long and in what manner their logs should be stored. Ensuring compliance is not only important for legal reasons but also essential for maintaining trust with customers and stakeholders.
- **Representation Across Network Segments:** Ensure that your log sources are not skewed towards a particular part of your network. Representation across all network segments is crucial for comprehensive visibility.

The objective is not to overwhelm your SIEM system with data, but to provide it with relevant data that can aid in threat detection and response. As such, your asset inventory, no matter how simple or extensive, should serve as a roadmap to achieving good log source coverage.

STRATEGY NO #6: DATA NORMALISATION AND ENRICHMENT

Data normalisation is a process that transforms disparate data formats into a unified, standard format. This is crucial because log data comes from various sources and in various formats. By normalising this data, a SIEM system can more easily correlate and analyse it.

Data enrichment, on the other hand, involves adding contextual information to log data. This could include information about the devices, users, applications, or network traffic associated with the data. Enriched data provides a more detailed view of activities, helping to improve the accuracy of threat detection and the effectiveness of response actions.

STRATEGY FOR DATA NORMALISATION AND ENRICHMENT

- **Assess Data Sources:** Understand the different types and formats of log data that your SIEM system is receiving. This will help you identify the requirements for data normalisation.
- **Develop a Normalisation Strategy:** Establish a standard format for each type of log data. This could involve defining a common set of data fields, or transforming data values to a standard format.
- **Implement Normalisation Rules:** Apply rules or scripts that transform incoming log data to the standard format. This could be done within the SIEM system, or in a separate data processing tool.
- **Identify Contextual Data:** Determine what additional information could add context to your log data. This could include data from asset management systems, threat intelligence feeds, or user databases.
- **Develop an Enrichment Strategy:** Define how and when to add contextual data to your log data. This could involve linking data based on IP addresses, user IDs, or other common identifiers.
- **Implement Enrichment Rules:** Apply rules or scripts that add contextual data to your log data. Again, this could be done within the SIEM system, or in a separate data processing tool.

CHECKLIST FOR DATA NORMALISATION AND ENRICHMENT

Proper data normalisation and enrichment are vital for effective SIEM optimisation. By standardising data formats and enriching log data with additional context, you can enhance your SIEM system's ability to accurately detect threats and respond to security incidents.

CHECKLIST ITEM	DONE
Understand the types and formats of log data	☐
Define a standard format for each type of log data	☐
Implement normalisation rules or scripts	☐
Identify potential sources of contextual data	☐
Define how to link contextual data with log data	☐
Implement enrichment rules or scripts	☐

STRATEGY NO #7: AUTOMATION AND ORCHESTRATION

Automation in a security context refers to the use of scripts, workflows, or automation platforms to perform routine, manual tasks without human intervention. This could include tasks such as data collection, normalisation, and alert generation. Automating these tasks can help to reduce errors, speed up processes, and free up time for security personnel.

Orchestration involves coordinating and integrating different automated tasks to work together effectively. This can help to streamline processes, ensure consistency, and improve the overall efficiency of security operations.

STRATEGY FOR AUTOMATION AND ORCHESTRATION

- **Identify Tasks for Automation:** Determine which routine, manual tasks can be automated. This might include tasks like data collection, normalisation, alert generation, and incident response tasks. Prioritise tasks that are time-consuming but require little decision-making.
- **Develop or Acquire Automation Scripts:** For each task that will be automated, develop scripts, workflows, or utilise automation platforms that can execute these tasks. This may require input from security analysts who are familiar with the tasks.
- **Test and Implement Automation:** Test the automation scripts or workflows in a controlled environment to ensure they work as expected. Once validated, these automations can be implemented.
- **Identify Dependencies and Sequences:** For orchestration, identify how different automated tasks depend on each other and the sequence in which they should occur. This could involve defining workflows.
- **Develop Orchestration Processes:** For each orchestrated workflow, define the process that will be followed. This might involve specifying the conditions under which certain tasks are triggered.
- **Test and Implement Orchestration:** Test the orchestration processes in a controlled environment to ensure they work as expected. Once validated, these can be implemented.

BEST PRACTICES FOR ONGOING SIEM OPTIMISATION

Optimising your SIEM system is a continuous journey, not a destination. It requires regular attention, adjustments, and fine-tuning to ensure it stays effective over time. Here are some best practices tailored for ongoing SIEM optimisation:

- **Commit to Continual Optimisation:** Recognise that SIEM is not a "set it and forget it" solution. Make regular optimisation a core part of your security strategy, allocating resources and time for this ongoing task.
- **Monitor and Refine:** Regularly assess your SIEM performance and make necessary adjustments. This includes fine-tuning rules based on the evolving threat landscape and your organisation's unique needs.
- **Continuous Learning and Training:** Ensure your security team is always updated on the latest SIEM features, threat intelligence, and incident response strategies. Ongoing training empowers them to leverage your SIEM system effectively.
- **Strengthen Vendor Relationships:** Keep lines of communication open with your SIEM vendor. They can provide valuable insights, access to updates, and new features that can boost your SIEM performance.
- **Embrace Automation:** Utilise automation for routine tasks to free up your team's time for strategic activities and reduce the possibility of human errors.
- **Maintain Comprehensive Documentation:** Keep a detailed record of all your SIEM activities and changes. This can support troubleshooting, audits, and new team member training.

The goal is to ensure your SIEM system stays agile, adaptable, and effective in an ever-changing cybersecurity landscape. Committing to the ongoing optimisation of your SIEM system is a key strategy in achieving this goal. The moment you decide to abandon this commitment, costs can start to spiral.

CONCLUSION

Implementing a SIEM system is a critical step towards enhancing your organisation's security posture. However, to unlock its full potential and ensure it provides the best possible protection, it's vital to commit to ongoing optimisation. By actively and continuously optimising your SIEM, you can better manage costs, reduce the number of false positives, maximise tool utilisation, adapt to organisational changes, and increase coverage for your assets.

SIEM optimisation is not a one-time task but a continuous process that requires commitment, time, skills, and a proactive approach. From the fine-tuning of rules and embracing automation, to fostering strong vendor relationships and maintaining comprehensive documentation, each strategy plays a crucial role in maintaining an agile, adaptable, and effective SIEM system.

The goal is not just to have a SIEM system, but to have a SIEM system that works effectively and efficiently for your unique needs. By integrating the principles and practices outlined in this guide, you can ensure your SIEM system remains a robust and reliable component of your cybersecurity strategy.